Gigamon®

CISO Insights

EXECUTIVE SUMMARY

Recalibrating Risk in the Age of AI

Introduction

CISOs are under mounting pressure as hybrid cloud environments grow more distributed, dynamic, and difficult to secure. As artificial intelligence (AI) advances digital transformation, it also introduces unprecedented complexity—outpacing the capabilities of conventional security and management tools. Internally, CISOs face unclear ownership of budgets and strategy, yet are still held accountable when things go wrong. As a result, **97 percent** of CISOs reveal they are making compromises in how they secure and manage their hybrid cloud infrastructure.

These compromises span everything from visibility gaps to data quality and tooling integration—foundational elements that CISOs know they can't afford to lose. The warning signs were already clear in 2024. Now, in 2025, the stakes have only grown higher. Breach rates are rising, AI threats are rapidly evolving, and the sheer volume of data is pushing conventional security tools to their limit. Traditional threat models no longer hold. Today's CISOs must recalibrate risk in real time, respond to emerging vulnerabilities, and lead at the intersection of visibility, control, and business strategy.

A new path is emerging. CISOs are turning to deep observability for the clarity required to move with speed, confidence, and precision. In this report, we examine how today's security leaders are adapting and what they must do to stay ahead of the curve going forward. We surveyed over 1,000 Security and IT professionals across Australia, France, Germany, Singapore, UK, and USA to publish our 2025 Hybrid Cloud Security Report: Recalibrating Risk in the Age of AI. The full report can be found here, but this executive summary presents key insights from 211 CISOs globally to uncover the critical challenges, compromises, and priorities shaping their role in today's AI-driven hybrid cloud landscape.

Compromises are being made across the board in these critical areas:

Ensuring security tools integrate and complement one another across on-prem, public and private cloud, including virtualized and container environments

Having comprehensive visibility across our entire IT infrastructure including lateral East-West traffic both on-prem and in the cloud

Having clean, accurate, and quality data to support deployment of new workloads including AI

Ensuring that network and application metadata is used to improve the effectiveness of security tools

Adopting a Zero Trust security framework and architecture

DEEP OBSERVABILITY DEFINED

The ability to efficiently deliver network-derived telemetry (packets, flows, metadata) to cloud, security, and observability tools that rely on MELT (metric, event, log, and trace) data. This powerful combination provides the deep observability organizations need to eliminate security blind spots, optimize network traffic, and lower the cost and complexity of securing and managing hybrid cloud infrastructure.

Cloud Perception is Shifting

CISOs are at the forefront of a major shift in how cloud risk is understood and managed. What was once considered an acceptable trade-off for agility is now being reassessed as a growing liability, particularly as AI adoption adds new layers of complexity.

In 2024, only **29 percent** of CISOs strongly agreed that cyber risk was rising due to rapid cloud migration. Now, in 2025, **75 percent** of CISOs say public cloud is a greater security risk than any other environment.

This is driving a re-evaluation of cloud strategies across the board. Nearly three-quarters (**73 percent**) of CISOs are considering repatriating data from public to private cloud, signaling a move toward regaining control over sensitive workloads. A third (**33 percent**) cite public cloud security and AI governance as top concerns, while over half (**54 percent**) are reluctant to deploy AI in public cloud environments due to security risk.

For CISOs, public cloud is no longer a default—it's a decision that demands scrutiny, strategy, and strong safeguards. This shift reflects a broader recalibration of risk in the AI era, where visibility and governance are non-negotiables. As hybrid cloud environments grow in complexity, CISOs are making more deliberate choices about where critical data and AI applications should reside, seeking not just performance, but security they can trust and control.

Data Quality is the Real Currency of Cybersecurity

CISOs have been down this road before. According to our survey, CISOs report an average of 15 security tools deployed across their environments, yet they've learned that the number of tools doesn't equate to the level of protection. The real challenge is integration: bringing high-quality, granular data together across tools to bring the complete picture into focus. In today's increasingly complex hybrid cloud environments, this level of deep observability allows CISOs to secure AI traffic, monitor systems effectively, and maximize the value of their existing investments.

CISO PERSPECTIVE

Eighty–six percent of CISOs agree that packet-level data and rich metadata are essential to strengthening their security posture, enabling faster, more accurate threat detection.

Tool integration is a challenge that many are still grappling with. For **1-in-3** CISOs (**32 percent**), having too many tools that are poorly integrated is a top concern, making it one of the most cited barriers to effective cybersecurity. The data explosion driven by AI is only intensifying the pressure, with **40 percent** of CISOs saying the volume of network data their tools must ingest and monitor has more than doubled in the past two years. In this context, the quality of data becomes a critical differentiator.

There are signs that progress is being made. Last year, **7-in-10** CISOs reported that their tools were ineffective at detecting breaches. This year, that number has dropped to **1-in-2** CISOs (**52 percent**), signaling that a shift toward optimizing existing tools—through higher quality data and tighter integration—is beginning to deliver results. While challenges remain, the trend suggests that CISOs are gaining traction by focusing on gaining complete visibility, not just adding incremental tools. In the age of AI, CISOs are redefining control through trusted, integrated data—gaining greater confidence in their ability to defend against continually evolving threats.

Critical Success Factors for CISOs

As AI complexity intensifies and expectations on CISOs continue to rise, success can't hinge on technical expertise alone. CISOs' success depends on a blend of strategy, operational clarity, and influence.

Leading the Charge on Secure AI Deployment

AI is no longer on the horizon—it's here. And CISOs are under pressure to secure and manage it, often without reliable infrastructure visibility or clear governance frameworks. In 2024, **59 percent** agreed more AI-specific education would help; in 2025, they're calling for practical solutions as AI implementation shifts into full-swing.

As they confront this shift, CISOs are focused on laying the foundations for secure AI deployment. Nearly half (**46 percent**) see deep observability as a top security priority when it comes to AI. Another **45 percent**

CISO PERSPECTIVE

Eighty–five percent now agree that deep observability is not just useful—it's a foundational element of hybrid cloud security.

are actively leveraging AI tools to enhance their own internal security capabilities. Monitoring is also rising on the agenda, with **39 percent** focused on improving data accuracy through closer oversight of AI applications. Meanwhile, **1-in-3** CISOs (**34 percent**) are implementing guardrails around large language models (LLMs), such as DeepSeek, to mitigate exposure to emerging risks.

AI implementation is no longer theoretical—CISOs are in execution mode. Success now hinges on practical frameworks that offer visibility and control to better secure and manage hybrid cloud infrastructure.

Visibility as the Differentiator

As AI accelerates complexity, visibility is emerging as a defining success factor for CISOs. The ability to monitor all data in motion, particularly lateral East-West traffic across hybrid environments, is what transforms fragmented signals into actionable intelligence. This priority is gaining urgency. This year, **83 percent** of CISOs reported they believe that effective cloud security depends on visibility into all data in motion. Yet nearly half (**48 percent**) say they still lack comprehensive visibility across their hybrid cloud infrastructure, particularly when it comes to lateral East-West traffic. As a result, real-time threat monitoring and visibility have become the top focus for **57 percent** of CISOs in the year ahead.

Visibility is more than a technical necessity. In a landscape overwhelmed by noise and fragmentation, achieving a state of clarity transforms reactive security into proactive defense, empowering organizations to anticipate and neutralize threats before they escalate.

Unlocking the Potential of the CISO-Board Partnership

Despite growing expectations, CISOs are still navigating unclear lines of ownership when it comes to cybersecurity strategy, decision-making, and funding. The disconnect is stark. While **52 percent** of CISOs believe they control the cybersecurity budget, only **8 percent** of their C-suite peers agree. This misalignment isn't just a communication issue—it's a structural one that leaves CISOs accountable for outcomes without the authority to influence the decisions that shape them.

The risks posed by AI are clear. It is crucial that CISOs remain on the offense and approach these threats in the same way malicious actors do. Strengthening cybersecurity defenses requires gaining deep observability into all data in motion to help understand where the gaps may be. By doing so, CISOs can better protect their hybrid cloud infrastructure against persistent threat actors seeking the perfect opportunity to strike.

CHAIM MAZAL
Chief Security Officer, Gigamon

As cybersecurity gains more prominence in the boardroom, this gap in perception and accountability is coming under increasing scrutiny. IT budgets still largely lie with CIOs and CTOs, limiting CISOs' ability to drive the programs they're responsible for securing. Yet the pressure continues to build. As a result, **81 percent** of CISOs agree that cybersecurity will soon carry the same level of accountability as financial or legal risk—that ultimately lands on their shoulders.

Bridging this gap starts with alignment across the leadership team. For **1-in-3** CISOs (**35 percent**), ensuring board-level awareness of AI's risks and benefits is seen as essential to achieving that alignment. And while **86 percent** now say deep observability is part of board-level cybersecurity conversations—up from **76 percent** in 2024—discussion doesn't always guarantee implementation. As AI drives cybersecurity further up in the business agenda, CISOs will need more than just a seat at the table. If they are to be accountable for mitigating business risk, they need the authority to shape how it's managed, and that shift begins by redefining their role as strategic partners at the board level.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

04.25_01